LiTH, Linköpings tekniska högskola
IDA, Institutionen för datavetenskap
Nahid Shahmehri

Written exam

TDDD17 Information Security

2009-06-09

14-18

Permissible aids

Dictionary (printed, NOT electronic)

Teacher on duty

David Byers, 013-282821, 0708282821

Instructions

There are 5 general questions and 5 in-depth questions. The general questions are from G1 to G5, and the in-depth questions are from D1 to D5. The questions are grouped pair-wise under their corresponding topic.

You have to answer at most 3 general questions and 3 in-depth questions. You must answer at least one of the questions for each topic. A correct answer for a general question gives you 2 points, and a correct answer for an in-depth question gives you 6 points. To pass the exam you need to accumulate at least 3 points from general questions and 9 points from in-depth questions. The exam grading depends on the total number of accumulated points.

Attention

If you answer more than 3 (general) + 3 (in-depth) questions we will randomly choose 3 + 3 answers for correcting the exam, while the rest of the answers will be discarded.

System Security

G1 What is the purpose of a "confidentiality policy"? Give an example of a security model that can be used to implement a confidentiality policy.

D1 Explain the purpose of the Bell LaPadula confidentiality model, and explain how the model works, including its interaction with discretionary access control. Be precise in your explanation. Explain at least one practical difficulty in employing the Bell LaPadula confidentiality model in a typical system.

Identification and Authentication

G2 The last few slides from the lectures on advanced user authentication treat some common mistakes and misconceptions about statistics. One point stressed there is that a FAR value for a piece of equipment does not necessarily give a correct value for the risk that an attacker manages to be accepted as another person. This is not something due to direct forgeries, like "gummy fingers", but a statistical phenomenon, which the attacker may be able to use. Describe this in just a few sentences.

D2 The course lists seven issues that should be studied and evaluated for any biometric property, which is to be used for identification or authentication of human users. Write down what you think are suitable requirement levels for each of these seven issues in a future ATM system! Then apply your criteria to fingerprints, iris scan and handwritten signatures, as an indication of their suitability in an ATM system. No absolute figures or technical details are required, but you should rank them as "best", "second best" and "least suitable" for each of the seven issues, with a short motivation for your ranking.

Network Security

G3 Firewalls are useful security devices, but the protection they offer is limited. Explain two likely ways in which a network protected by a firewall could be successfully attacked by an outsider.

D3 In the context of network security, a security domain is a network of systems that share a specified security level through a common element. In other words, they share a trust relationship.

a) Give two different concrete examples of security domains.

b) Explain why it is dangerous to create overlapping (i.e. combining) security domains.

c) How can risk assessment be used to identify security domains?

Risk Analysis

G4 How can an error message reveal the information about a system. Give an example.

D4 What is Hazard analysis and when is it useful? Perform a hazard analysis for systematic failure of a fire alarm system.

Business Continuity Planning, Physical Security

G5 Define disaster and non-disaster in the context of a BCP.

D5 List and describe three requirements on a BCP.